(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 047 215 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.10.2000 Bulletin 2000/43

(51) Int. Cl.[7]: **H04J 11/00**

(21) Application number: **00303039.2**

(22) Date of filing: **11.04.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.04.1999 US 294165**

(71) Applicant:
LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventors:
- **Giardina, Charles Robert**
  Mahwah, New Jersey 07430 (US)
- **Rudrapatna, Ashok N.**
  Basking Ridge, New Jersey 07920 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) A method of enhancing security for the transmission of information

(57) Quasi-Walsh function systems are developed which allow multiple access as well as spectral spreading for interception and jamming prevention. Mutual interference is minimal due to orthogonal spreading. High signal hiding capability occurs by utilizing a large number of distinct orthogonal codes. An encoding algorithm is presented which allows a simple way of "keeping track" of the different systems of Quasi-Walsh systems as well as determining appropriate values for given users at specified chip values.

FIG. 2

20

$$\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = H^{*}D0 = Q0 = \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = H^{*}D1 = Q1 = \begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} = H^{*}D2 = Q2 = \begin{pmatrix}-1 & 1\\ -1 & -1\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = H^{*}D3 = Q3 = \begin{pmatrix}-1 & -1\\ -1 & -1\end{pmatrix}$$

EP 1 047 215 A2

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

FIELD OF THE INVENTION

[0001] The present invention relates generally to wireless communications systems and, in particular, to wireless communications systems based on code division multiple access (CDMA).

BACKGROUND OF THE RELATED ART

[0002] The well known system of Walsh Hadamard functions H (of length 2^n, where n is a positive integer) form an orthogonal basis for the Euclidean space $R2^n$ and have range one and minus one. These functions have found application in the CDMA area for wireless communication. More recently, systems of Quasi-Walsh functions Q were introduced for application in CDMA wireless communication systems. These functions, having similar properties as the Walsh functions, also form an orthogonal basis for $R2^n$ and attain only values one and minus one. The systems of Quasi-Walsh functions are formed by negating arbitrarily specified tuples of Walsh Hadamard functions. In terms of matrix operations, the systems of Quasi-Walsh functions Q are row vectors obtained by post multiplying the Walsh Hadamard matrix H by a diagonal matrix D, which is comprised of ones and minus ones — i.e., $Q = H D$. Note that the values in each row vector represents a chip. This matrix representing Quasi-Walsh functions Q is a length preserving transformation called an isometry, or an orthonormal transformation, in this case where the underlying field is real valued. Since the Walsh Hadamard matrix is orthogonal along with the diagonal matrix D, the resulting product matrix Q is also orthogonal. Accordingly, distinct row vectors in Q, i.e., distinct Quasi-Walsh functions, have an inner product of zero. Note that when the diagonal matrix D is an identity matrix I, the Walsh Hadamard matrix appears. Therefore, Walsh Hadamard matrix H is a special case of the Quasi-Walsh matrix when D=I .

SUMMARY OF THE INVENTION

[0003] The present invention utilizes systems of Quasi-Walsh functions for high resilience against interception and jamming in addition to allowing multiple access and acquisition. The present invention switches among generalized systems of Quasi-Walsh functions at some rate *r*, where *r* may either be a fixed or variable value not equal to zero. The present invention transmits a first set of information for a user over a communication channel using a first code, and transmitting a second set of information for the user over the communication channel using a second code in place of the first code, wherein the first and second codes may be orthogonal codes or encryption codes and the communication channel has a fixed or variable data rate.The first and second codes may be indicated using an index, such as a pseudo-random sequence, an algorithm, a mathematical equation, a known or cyclical sequence, etc., wherein the index may be single or multi-valued. In one embodiment, the first and second codes correspond to row vectors *i* and *j* in a first and second systems of orthogonal functions. The row vectors *i* and *j* may be identical or different in their respective systems of orthogonal functions. Likewise, the first and second systems of orthogonal functions may be identical or different, and may be systems of Quasi-Walsh functions.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The features, aspects, and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where

FIG. 1 depicts an example of four possible diagonal matrices D_k;
FIG. 2 depicts an example of four possible systems of Quasi-Walsh functions Q_k derived using the diagonal matrices D_k of FIG. 1; and
FIG. 3 depicts an example of two chips used for modulating each bit being transmitted.

DETAILED DESCRIPTION

[0005] To begin, it will be assumed that a chipping rate of 2^n chips per information bit is employed although other chipping rates are possible. Accordingly, a standard $2^n x 2^n$ Q matrix will be utilized throughout. As usual in CDMA applications, each user is assigned a specific row in the Q matrix, thereby allowing multiple access in the data channel. If more than $2^n x 2^n$ users are desired, rows in a another Q matrix are designated to the additional users. In the latter case, the other Q matrix is chosen such that mutual interference is minimal. However, as before, it cannot be zero due to the non-orthogonality between any two systems of Quasi-Walsh functions Q. Generalization to arbitrary frames of systems of Quasi-Walsh functions Q is immediate. In the ensuing paragraphs, emphasis is placed on cases with no more than 2^n users. But it should be understood that the present invention is also applicable to more than 2^n users.

[0006] For convenience, the i^{th} user will be assigned the i^{th} row vector (or i^{th} Quasi-Walsh function in a system of Quasi-Walsh functions) in Q for the first bit transmitted. Throughout, it is assumed, with the help of the pilot and synch channels, that perfect synchronization exists. Subsequently, the i^{th} user will be assigned the i^{th} row in distinct Q matrices, which are generated bit by bit. With each bit k transmitted, a diagonal matrix D_k is found using a pseudo random number generator. See FIG. 1 depicting an example of four possible diagonal matrices D_k, where k=0,1,2,3. The number of possible distinct matrices is

2^{2^n}.

Moreover, the same D_k can occur numerous times in a single realization, thereby making a potentially large period for a resulting Pseudo Noise (PN) type sequence. The unique matrix D_k, post-multiplies H to give $Q_k = H D_k$. See FIG. 2 depicting an example of four possible systems of Quasi-Walsh functions Q_k derived using the diagonal matrices D_k of FIG. 1. Accordingly, the i^{th} user is provisioned always the same i^{th} row, however, it very likely comes from different Quasi-Walsh systems for each information bit transmitted. To an observer without knowledge of the formula for isometry generation, the resulting string of Quasi-Walsh functions seems random, thus hard to intercept.

[0007] Generalization to support larger than 2^n users is straightforward. We illustrate here the approach for supporting $2^{(n+1)}$ users; generalization to support users in excess of this follows the same logic. For each bit k, two D matrices are chosen, D_k^1 and D_k^2 such that all the Quasi-Walsh functions they produce are "almost orthogonal" with each other. The first 2^n users will be assigned Quasi-Walsh functions from Q_k^1 as described before and the next 2^n users from Q_k^2.

[0008] For any specific bit, the i^{th} user is assigned the i^{th} row involving Quasi-Walsh functions Q_k, whereas the b^{th} user is assigned the b^{th} row involving the same Quasi-Walsh functions Q_k. As a consequence, no mutual interference occurs since these codes are orthogonal. Thus, just like in a maximal length large shift register PN sequence, a long Quasi-Walsh type PN sequence can result across successive bits. This sequence of successive bits has all the signal hiding benefits as does a shift register sequence. In other words, the Quasi-Walsh functions Q_k are changed across successive bits using an index, wherein the index may be determined using a PN sequence, an algorithm, a mathematical function, a known sequence, etc. Additionally, it has the added benefit of orthogonality resulting in ease of multiple access and acquisition. The length of the Quasi-Walsh PN sequence, before it repeats is a function of the length of the random number generator each of which determines the isometry of D_k. As an added degree of randomness the i^{th} user at each bit may use a row other then the i^{th}. The actual row involving the Quasi-Walsh functions Q_k can change (using another pseudo random number generator).

[0009] For a given $2^n x 2^n$ Walsh Hadamard matrix H,

2^{2^n}

distinct systems of Quasi-Walsh functions occur due to post multiplication by distinct diagonal isometrics D_k. The diagonal entries in these matrices will be interpreted in binary by replacing the minus ones on the diagonal by zeros. As a result, each distinct D_k can be represented by an integer between 0 and

$(2^{2^n} - 1)$.

Thus encoding, and correspondingly the decoding can be efficiently represented by the specific index k associated with each bit.

[0010] As a simplified illustration, consider the following example. In R2, two chips are used per single bit of information, and two users will be considered. In this case, n =1. Four distinct diagonal orthogonal matrices arise, as shown earlier in FIG. 1. When each of these matrices D_k are applied to the Walsh-Hadamard matrix H by post multiplication, the systems of Quasi-Walsh functions Q_k shown in FIG.2 are found.

[0011] To illustrate that for any realization consisting of all possible diagonal matrix isometrics an equal number of ones and minus ones occur, consider the following. Referring to the previous illustration, for each of the four bits of information transmitted, a diagonal matrix isometry is utilized. Suppose that an index specifics the isometrics D_k in the following order: D_0, D_1, D_2, and D_3. Accordingly, the two chips used for modulating each bit transmitted are shown in FIG. 3. Note the equal number of 1 and —1 combinations both for User0 and User1.

[0012] The present invention is applicable to both Sylvester and non-Sylvester types. This permits operating in a non 2^n (n, integer) Real space The present invention is also applicable among non-orthogonal systems of Quasi-Walsh functions Q. Post multiplying Q by a permutation matrix P yields a generalized system of Quasi-Walsh function Q^G, i.e., $Q^G = H D P$. Note that here P has the same dimension (i.e., mxm) as H and D. Since, there are m! distinct Ps, the overall system of Q^G increases by m! when compared to the system of Quasi-Walsh functions Q, improving the probability of finding cross system, low correlation generalized system of Quasi-Walsh functions, thereby yielding minimum mutual interference.

[0013] The process described above for assigning Quasi-Walsh functions works in the same manner for generalized systems of Quasi-Walsh functions Q^G, where $Q^G{}_j = H D_k P_x$. Where k = 1 to m (not necessarily equal to 2^n) and x = 1 to m ! Thus the specific generalized systems of Quasi-Walsh functions is defined by j, which is a function of the two-valued tuple {k, x}. Thus information hiding can be accomplished by the two-dimensional index or tuple {k, x}, enhancing information-hiding properties. In one realization, as described above each user would use the same specific row vector across all bits with each user using a different row with respect to each other. In this specific realization, spreading sequence for bit j would be selected from $Q^G{}_j$. Thus encoding, and correspondingly the

decoding can be represented by the specific index j [or the tuple {k, x}] associated with each bit.

Claims

1. A method of transmitting information comprising the steps of:

   transmitting a first set of information for a user over a communication channel modulated using a first code and
   transmitting a second set of information for the user over the communication channel modulated using a second code in place of the first code.

2. The method of claim 1 comprising the additional step of:

   transmitting a third set of information for the user over the communication channel modulated using a third code in place of the second code.

3. The method of claim 2, wherein the communication channel has a fixed or variable data rate.

4. The method of claim 1, wherein the first and second codes are indicated using an index.

5. The method of claim 1, wherein the first code corresponds to a row vector *i* in a first system of orthogonal functions and the second code corresponds to a row vector *j* in a second system of orthogonal functions.

6. The method of claims 5, wherein the row vector *i* and the row vector *j* are a same row in their respective system of orthogonal functions.

7. The method of claim 5, wherein the row vector *i* and the row vector *j* are different rows in their respective system of orthogonal functions.

8. The method of claim 5, wherein the first system of orthogonal functions is not identical to the second system of orthogonal functions.

9. The method of claim 5, wherein the first system of orthogonal functions is identical to the second system of orthogonal functions.

10. The method of claim 5, wherein the first and second systems of orthogonal functions are generalized systems of Quasi-Walsh functions.

11. The method of claim 5, wherein the row vector I and the row vector j are defined using an index.

12. The method of claim 5, wherein the first and second systems of orthogonal functions are defined using an index.

13. The method of claim 1, wherein the first set of information corresponds to a bit n and the second set of information corresponds to a bit n+r, where r is a fixed value not equal to zero.

14. The method of claim 1, wherein the first set of information corresponds to a bit n and the second set of information corresponds to a bit n+r, where r is a variable value not equal to zero.

15. A method of transmitting bits for an ith user comprising the steps of:

   assigning an ith row vector to the ith user;
   transmitting a bit n associated with the ith user using the ith row vector in a first system of orthogonal functions;
   transmitting a bit n+r associated with the ith user using the ith row vector in a second system of orthogonal codes, wherein the first system of orthogonal codes is not identical to the second system of orthogonal functions.

16. The method of claim 15, wherein the first and second systems of orthogonal codes are generalized systems of Quasi-Walsh functions.

17. The method of claim 15, wherein the first and second systems of orthogonal codes are indicated using an index.

18. The method of claim 4,11,12 or 17, wherein the index is defined by a psuedo-random number sequence.

19. The method of claim 4,11,12 or 17, wherein the index is defined by an algorithm.

FIG. 1

10

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = D0$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = D1$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = D2$$

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = D3$$

FIG. 2

20

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = H^*D0 = Q0 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = H^*D1 = Q1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = H^*D2 = Q2 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = H^*D3 = Q3 = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

FIG. 3

30

FOR USER 0: [1 1], [1 -1], [-1 1], [-1 -1]

FOR USER 1: [1 -1], [1 1], [-1 -1], [-1 1]

Bit 1 Bit 2 Bit 3 Bit 4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 047 215 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
05.11.2003 Bulletin 2003/45

(43) Date of publication A2:
25.10.2000 Bulletin 2000/43

(21) Application number: **00303039.2**

(22) Date of filing: **11.04.2000**

(51) Int Cl.[7]: **H04J 11/00**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.04.1999 US 294165**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventors:
- **Giardina, Charles Robert**
  Mahwah, New Jersey 07430 (US)
- **Rudrapatna, Ashok N.**
  Basking Ridge, New Jersey 07920 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) A method of enhancing security for the transmission of information

(57) Quasi-Walsh function systems are developed which allow multiple access as well as spectral spreading for interception and jamming prevention. Mutual interference is minimal due to orthogonal spreading. High signal hiding capability occurs by utilizing a large number of distinct orthogonal codes. An encoding algorithm is presented which allows a simple way of "keeping track" of the different systems of Quasi-Walsh systems as well as determining appropriate values for given users at specified chip values.

FIG. 2

20

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = H^{*}D0 = Q0 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = H^{*}D1 = Q1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = H^{*}D2 = Q2 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = H^{*}D3 = Q3 = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

EP 1 047 215 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 3039

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 771 288 A (BOTTOMLEY GREGORY E ET AL) 23 June 1998 (1998-06-23) * column 21, line 7 - line 10 * * column 21, line 41 - line 55 * * column 25, line 26 - line 47 * * figure 9 * ---	1-19	H04J11/00
X	US 5 515 396 A (KOTZIN MICHAEL D) 7 May 1996 (1996-05-07) * column 3, line 58 - line 63 * * column 5, line 14 * * column 5, line 27 - line 51 * * column 6, line 47 - line 50 * * figure 2 * -----	1-19	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04J

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	2 September 2003	Fouasnon, O

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 3039

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

02-09-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5771288 A	23-06-1998	US 5742678 A	21-04-1998
		US 5550809 A	27-08-1996
		US 5353352 A	04-10-1994
		AU 1214499 A	04-03-1999
		AU 703405 B2	25-03-1999
		AU 3322095 A	07-03-1996
		BR 9508876 A	30-12-1997
		CA 2197640 A1	22-02-1996
		CN 1159872 A ,B	17-09-1997
		EP 0776555 A1	04-06-1997
		FI 970637 A	11-04-1997
		JP 10507322 T	14-07-1998
		NO 970667 A	16-04-1997
		RU 2160508 C2	10-12-2000
		WO 9605668 A1	22-02-1996
		AU 4026993 A	18-11-1993
		BR 9305479 A	11-10-1994
		CA 2110995 A1	28-10-1993
		DE 69330445 D1	23-08-2001
		DE 69330445 T2	02-05-2002
		EP 0565506 A2	13-10-1993
		ES 2162810 T3	16-01-2002
		FI 935526 A	14-01-1994
		HK 1014321 A1	28-03-2002
		JP 6511371 T	15-12-1994
		MX 9301960 A1	01-10-1993
		NZ 251900 A	28-10-1996
		SG 43043 A1	17-10-1997
		WO 9321709 A1	28-10-1993
US 5515396 A	07-05-1996	CA 2158356 A1	31-08-1995
		EP 0705500 A1	10-04-1996
		FI 955063 A	24-10-1995
		JP 8509591 T	08-10-1996
		WO 9523459 A1	31-08-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82